REFERENCES

[1] A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, Dec. 1999.

[2] A. Freier, P. Kariton, and P. Kocher. The SSL protocol: Version 3.0. Internet draft, NetscapeCommunications, 1996.

[3] A. Genkina, A. Friedman, and J. Camp. Net trust. Trustworthy Interfaces for Passwords and Personal Information (TIPPI) Workshop, June 2005.

[4] A. Herzberg and A. Gbara. Trustbar: Protecting (even naive) web users from spoofing and phishing attacks. Cryptology ePrint Archive, Report 2004/155, 2004.

[5] Ang, L., C. Dubelaar, & B. Lee. To Trust or Not toTrust? A Model of Internet Trust From the Customer'sPoint of View. *Proc. 14th Bled E-Commerce Conf.* (2001), 25-26.

[6] Anti-Phishing Working Group. *Phishing Activity Trends Report November 2005* (2005).

[7] Anti-Phishing Working Group. Phishing activity trends report. , Aug. 2005.

[8] Ba, S. & P. Pavlov. Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior. *MIS Quarterly*, 26, 3(2002), 243-268.

[9] Dhamija, R. & J. D. Tygar. The Battle Against Phishing: Dynamic Security Skins. *Proc. SOUPS* (2005).

[10] Dhamija, R. Authentication for Humans: The Design and Analysis of Usable Security Systems. Ph.D.Thesis, University of California Berkeley (2005).

[11] Ecommerce Times By: Harbaksh Singh Nanda Date: December 23, 2004

[12] Egger, F.N. Affective Design of E-commerce User Interfaces: How to Maximize Perceived Trustworthiness. *Proc. Intl. Conf. Affective Human Factors Design* (2001), 317-324.

[13] Erhel, S. and E. Jamet. 2006. Using pop-up windows to improve multimedia learning. *Journal of Computer Assisted Learning*, Volume 22, Number 2. pp. 137 - 147.

[14] FDIC. Authentication in an internet banking environment. Technical Report FIL-103-2005, Federal Deposit Insurance Corporation, Oct. 2005.

[15] Federal Trade Commission. An E-Card for You game. Retrieved December 30, 2006.

[16] Federal Trade Commission. Phishing Alerts. Retrieved December 30, 2006.

[17] Ferguson, A. J. 2005. Fostering E-Mail Security Awareness: The West Point Carronade. *EDUCASE Quarterly*

[18] Fette, I., N. Sadeh and A. Tomasic. Learning to Detect Phishing Emails. June 2006. ISRI Technical report, CMUISRI- 06-112.

[19] Fogg, B. J. et al. How Do Users Evaluate the Credibility of Web Sites?: A Study with Over 2,500 Participants. *Proc. DUX* (2003).

[20] Fogg, B. J. Stanford Guidelines for Web Credibility. *Res. Sum. Stanford Persuasive Tech. Lab.* (2002).

[21] G. Goth. Phishing attacks rising, but dollar losses down. *IEEE Security and Privacy*, 3(1):8, January–February 2005.

[22] Jagatic, T.,N. Johnson, M. Jakobsson and F. Menczer. Social Phishing. To appear in the *Communications of the ACM*. Retrieved March 7, 2006,

[23] Kim, D., Y. Song, S. Braynov, & H. Rao. A B-to-C Trust Model for Online Exchange. *Proc. AmericasConf. on Inf. Sys*. (2001), 784-787.

[24] Kumaraguru, P., A. Acquisti and L. Cranor. 2006. Trust modeling for online transactions: A phishing scenario. *Proceedings of Privacy Security Trust*, Oct 30 - Nov 1, 2006, Ontario, Canada

[25] Lee, M. & E. Turban. A Trust Model for Consumer Internet Shopping. *Intl J. Elec. Commerce*, 6, 1, (2001), 75-91.

[26] Lininger, R. and R. Dean. 2005. *Phishing: Cutting the IdentityTheft Line.* Wiley, publishing Inc. Indianapolis, Indiana, USA.

[27] Litan, A. *Phishing Attack Victims Likely Targets forIdentity Theft*. Gartner Research (2004).

[28] M. Jakobsson and A. Young. Distributed phishing attacks. Workshop on Resilient Financial Information Systems, Mar. 2005.

[29] M. Jakobsson. Modeling and preventing phishing attacks. In *Financial Cryptography*, 2005.

[30] M. McCune, A. Perrig, and M. K. Reiter. Seeing is believing: Using camera phones for humanverifiable authentication. In *IEEE Symposium on Security and Privacy*, May 2005.

[31] Mail Frontier. Phishing IQ.http://survey.mailfrontier.com/survey/quiztest.html. RetrievedSept 20, 2006

[32] Mayer, R.E. and R. B. Anderson. 1991 Animations Need Narrations: An Experimental Test of a Dual Coding Hypothesis. *Journal of Educational Psychology*. Volume 83, Number 4. pp. 484 – 490.

[33] N. Chou, R. Ledesma, Y. Teraguchi, D. Boneh, and J. C. Mitchell. Client-side defense againstweb-based identity theft. In *NDSS*, Feb. 2004.

[34] N. Haller. The S/Key one-time password system. In *Proceedings of the Symposium on Network and Distributed Systems Security*, pages 151–157, Feb. 1994.

[35] P.MacKenzie andM. K. Reiter. Networked cryptographic devices resilient to capture. *InternationalJournal of Information Security*, 2(1):1–20, Nov. 2003.

[36] Phishing Cutting the Identity Theft Line, Rachael Lininger and Russell Dean Vines, Wiley Publishing, Inc. 2005

[37] R. Clayton. Who'd phish from the summit of kilimanjaro? In *Financial Cryptography*, pages 91–92, 2005.

[38] R. Dhamija and J. D. Tygar. Phish and HIPs: Human interactive proofs to detect phishing attacks.In *Human Interactive Proofs: Second International Workshop (HIP 2005)*, May 2005.

[39] R. Dhamija and J. D. Tygar. The battle against phishing: Dynamic security skins. In *ACM Symposium on Usable Security and Privacy (SOUPS '05)*, July 2005.

[40] T. Dierks and C. Allen. The TLS protocol version 1.0. Internet Request for Comment RFC 2246,Internet Engineering Task Force, Jan. 1999. Proposed Standard.